EXHIBIT 23

Miercom

Cisco Systems Digital Network Architecture
vs
Huawei Agile Campus

DR170921G

October 2017

Miercom
www.miercom.com

Contents

1 - Executive Summary

Miercom was engaged by Cisco Systems to independently configure, operate and assess aspects of campus-scale, wireless and wired network infrastructures from Cisco Systems and Huawei Technologies. The products of each vendor were configured and deployed strictly according to the vendors' recommended designs, and using their respective software for campus-wide network management, control, configuration and monitoring.

Tests were conducted in two main areas:

1. **Wireless:** Focusing on client density, throughput, radio and interference management, application support and visibility, device profiling, high availability, and security.
2. **Wired:** Evaluating switches on their ability to perform rich traffic analysis and encrypted threat detection, security and optimization of hardware resources, power stacking and high availability for growing IoT devices enabled by PoE, programmability.

Key Findings and Observations:

- **Better radio management**. In serving the same 180-client high wireless test network, Huawei's APs (AP7050DE's) adjusted transmit power that was overbearing for a high density deployment, at nearly twice the strength, on average, of Cisco's APs (2802i's); too-strong signals lead to interference and client-connectivity issues. Also, client connectivity was more evenly distributed among Cisco APs than Huawei's. In addition, Cisco's APs automatically switched their 2.4-GHz radios to operate at 5 GHz, better optimizing client coverage – an impressive capability that the Huawei APs do not support.

- **More wireless throughput and quality video sessions**. Configured in the same, dual-mode 2.4/5-GHz manner, Cisco's APs enabled clients to achieve up to 22 percent more bi-directional TCP-traffic throughput than Huawei's. Also, Huawei exhibited occasional packet loss with failure to transmit to certain clients, where Cisco did not, even with all 180 clients active. We observed, too, that given the same traffic, Cisco APs support more quality client video sessions than Huawei.

- **Better identification of traffic, client devices, and interference sources.** Cisco could identify many contemporary traffic types that Huawei could not, including Instagram, Dropbox and WebEx. Cisco could also correctly identify all interference sources that we applied, while Huawei could partially identify only one.

- **Higher availability, faster fail-over**. In their fault-tolerant configurations, Cisco could restore a failed link and wireless controller much faster than Huawei. Time-dependent apps like video continued uninterrupted with Cisco, but timed out with Huawei. Also, Cisco's wireless and wired infrastructure supports various power options, including pooled and shared power supplies, perpetual and Fast Power-over-Ethernet, which assure that powered network devices experience minimal or no power interruptions.

- **Security without losing performance**. Many security processes in the Cisco environment, including DTLS encryption, are implemented in hardware, while the same processes are done in software by Huawei which detracts from the processing capacity available for traffic handling.

- **Encrypted Traffic Analytics**. From basic visibility to robust security, Cisco successfully delivers innovative tools for enterprises to identify application flows, offer strong security and compliances to their network infrastructure even for threats from malware, botnets etc. hidden inside encrypted traffic, without compromising privacy. Huawei solutions lack the same level of visibility and security required for modern application and threats.

- **Secured and optimized hardware resources**. The Catalyst switching resources supported high-speed policy edits (add/delete) with efficient resource allocation for scale and secure implementation. With features such as "ACL Label-Sharing" and "Hitless ACL updates", the switches demonstrated programming of policy to the network without being compromised. We observed that the Huawei switches can "leak" data that should be blocked while its ACL changes are being propagated and applied to each switch interface.

- **High Availability for PoE devices**. Cisco Stack-Power offers unique advantages over Huawei by pooling power supplies from the individual sources to enable resiliency. Cisco Fast PoE and Perpetual PoE offers high availability to all the PoE connected device when device reboots, either intentionally or unintentionally

- **Software Programmability.** Cisco IOS-XE Programmability support technologies that simplify automation and provisioning and make the network engineer more efficient. IOS-XE has the ability to host Linux based applications via their Guest Shell feature which can provide a number of valuable use cases for the network infrastructure.

- **Trustworthiness.** Cisco trustworthy systems establish the base of assurance for an architected secured network. Cisco secures and protects network by using image signing, secure boot, trust anchor module, runtime defenses and control plane security.

Based on the results of this testing, comparing the campus wired and wireless network architectures and wares of Cisco and Huawei Technologies, we found many businesses enabling capabilities favoring the Cisco solution. We proudly award the ***Miercom Performance Verified Certification*** to Cisco's campus-infrastructure network designs and related packages for monitoring, management and control.

Robert Smithers
CEO
Miercom

2 – How We Did It

Two campus-infrastructure networks were assembled side-by-side for this testing – one Cisco Systems', one Huawei Technologies'. The key component parts of each are detailed below. Miercom engineers ensured that the competitive topologies, all the products and their configurations, represented the latest and most appropriate apples-to-apples offerings from both Cisco and Huawei. The wireless tests discussed in this report were conducted in a facility configured and used solely for testing wireless equipment.

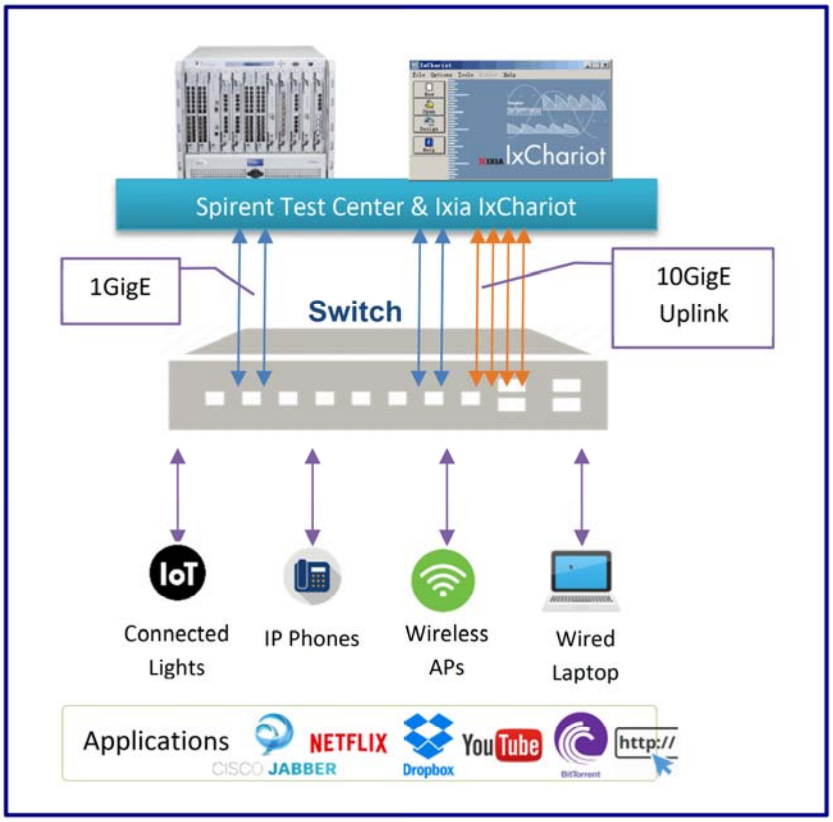
Products Tested

	Cisco Systems		Huawei Technologies	
Equipment	**Model**		**Model**	
Access Points	2802i 	List price: $1,295 Radio: 4x4:3 MU-MIMO Channel width: 160 MHz Ethernet: 2xGbE	AP7050DE 	List price: $1,295 Radio: 4x4:4 MU-MIMO Channel width: 160 MHz (2x2) Ethernet: 2xGbE
	Model	**Software**	Model	**Software**
Wireless Controller	5520	V8.3 MR3	AC6605	V200R700C20SPC200
Switch	Catalyst 3850	V16.6.1	S5720 HI	V2R11
Switch	Catalyst 9300	V16.6.1	S5720 HI	V2R11
Switch	Catalyst 2960XR	V15.2.6	S5720 SI	V2R11

Test Tools

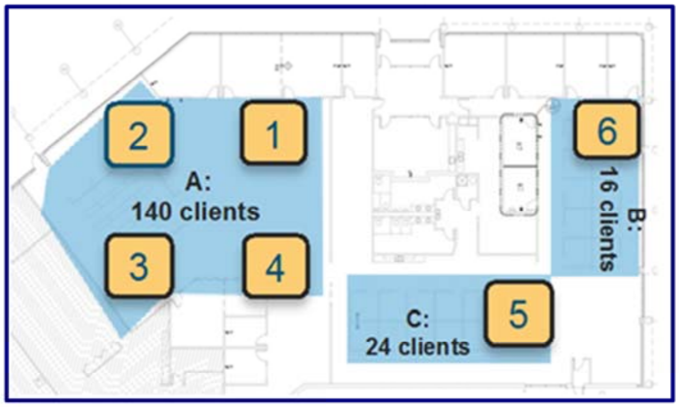
Test Tool	Version
Ixia IxChariot	V7.3
Spirent Test Center	V4.6.7

Test Setup 1: Switching



Source: Cisco

Test Setup 2: Wireless



Source: Miercom

For testing client density, signal power and throughput performance, six of each vendor's APs were deployed, numbered as shown in the below diagram. A total of 180 clients were set up on tables throughout the three areas shown in blue. Area A was a large open room with 140 clients on tables. Areas B and C with 16 and 24 clients, respectively, were rooms with office partitions containing 1 to 2 clients per cubicle.

To reflect the industry Wi-Fi movement from 2.4 GHz radio operation and towards 5-GHz, the majority of clients, 140 or 78 percent, operated at 5 GHz and the remaining 40 clients, or 22 percent, operated on 2.4 GHz band.

Each client's Wi-Fi supported a mix of standards: IEEE 802.11n (20), IEEE 802.11ac (120), and IEEE 802.11ac Wave 2 (40). The clients, and their varying capabilities, including clients supporting 802.11ac Wave 2 with Multi-user MIMO were chosen to emulate real world environments.

Client	WiFi Support, No. of Spatial Streams, MIMO Support	No. of Clients
MacBook Pro	11ac, 3SS, SU-MIMO	50
MacBook Air	11ac, 2SS, SU-MIMO	20
Dell E6430 w/ Broadcom43460	11ac, 3SS, SU-MIMO	10
Dell E6430 w/ Intel 7260	11ac, 2SS, SU-MIMO	30
Acer Aspire	11ac, 1SS, MU-MIMO	30
Dell E5450	11ac, 2SS, MU-MIMO	10
MacBook Pro	11n, 3SS, SU-MIMO	10
iPad Air	11n, 2SS, SU-MIMO	10
Apple iPhone 6	11ac, 1SS, SU-MIMO	10

3 – Wireless

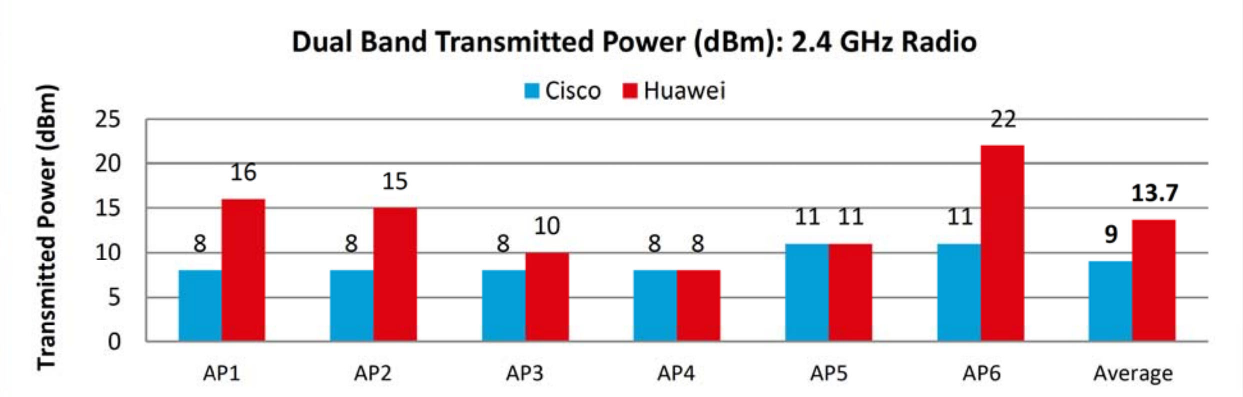
AP Transmit Power Levels

Three different AP environments were tested:

1. Huawei "Dual Band," where each of the six APs ran a 2.4 and a 5 GHz radio;
2. Cisco "Dual Band," where each of the six APs ran a 2.4 and a 5 GHz radio; and
3. Cisco "Dual 5 GHz." This uses a unique Cisco feature, where an AP can "flip" its 2.4 GHz radio to operate at 5 GHz, depending on the overlapping coverage in the 2.4 GHz band. In this third scenario, two of Cisco's six APs (numbers 1 and 4 on the layout diagram), flipped their 2.4-GHz radios and operated both their radios at 5 GHz.

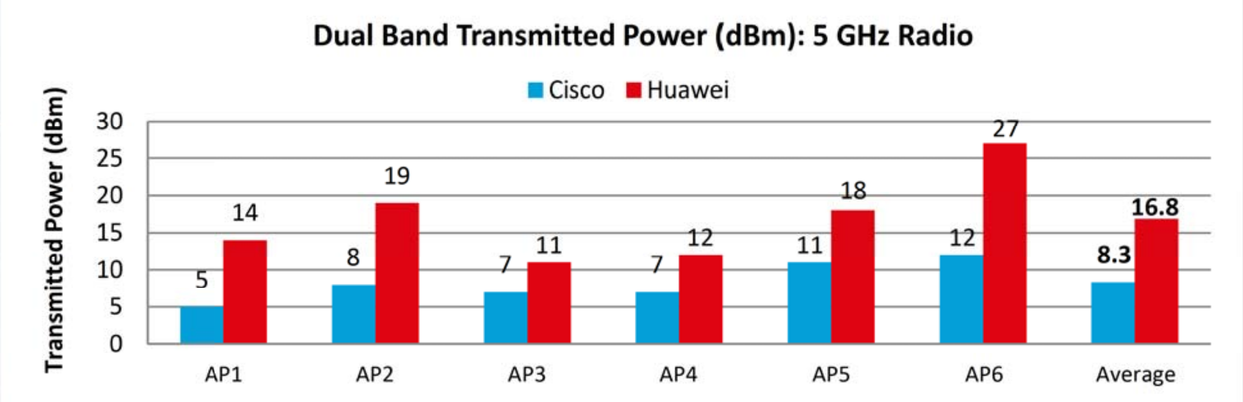
The following graphs show the per-channel transmitted power levels for these environments.

Dual Band 2.4 and 5 GHz Radio: Cisco vs Huawei



Source: Miercom

Cisco operated as low as 8 dBm. Its average transmitted power was 4.7 dBm lower than Huawei.

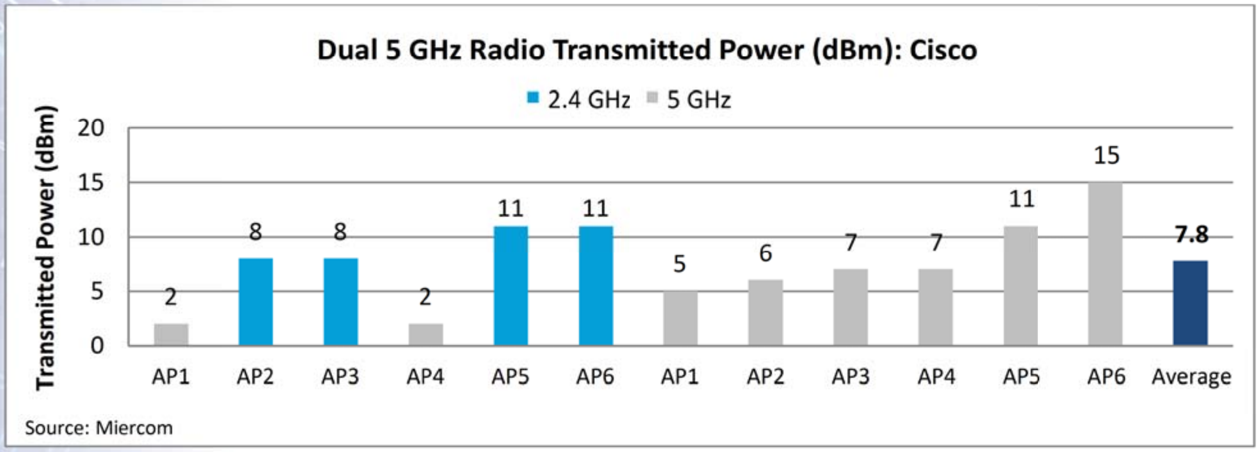


Source: Miercom

Cisco operated as low as 8.3 dBm. Its average transmitted power was 8.5 dBm lower than Huawei.

Huawei's transmit levels for dual band averaged 15.25 dBm (decibels referenced to one milliwatt). One Huawei AP operated at full transmit power (27 dBm). By comparison, the Cisco dual-band APs averaged just 8.67 dBm per transmit channel, about half of Huawei's average transmit-power.

Dual Band 5 GHz Radio: Cisco



Source: Miercom

We found the lowest AP transmitted power, averaging just 7.8 dBm, with the Cisco Dual 5 GHz environment.

Cisco Channel and Power Configuration per Radio

AP	Channel	Radio	Power (dBm)
AP1	36+	5 GHz	2
	100+	5 GHz	5
AP2	1	2.4 GHz	8
	64-	5GHz	6
AP3	11	2.4 GHz	8
	149+	5 GHz	7
AP4	128-	5 GHz	2
	44+	5 GHz	7
AP5	6	2.4 GHz	11
	161-	5 GHz	11
AP6	11	2.4 GHz	11
	108+	5 GHz	15

High AP transmit-power levels can create co-channel interference and lead to "sticky clients." This is where clients won't roam because the AP's signal is too strong, but the client's signal is too weak to reliably reach the AP.

Client Distribution

Both vendors' APs were positioned the same, and clients were never moved during the testing. Still, the distribution of clients connecting to the six APs was notably different, even with vendor client load balancing techniques in use.

While client distribution favors their proximity to the closest AP, we expected a more even distribution. A common scenario of too many clients on one AP slows throughput while other nearby APs are underutilized. The table shows the number of 5-GHz clients that automatically connected to the vendors' six APs.

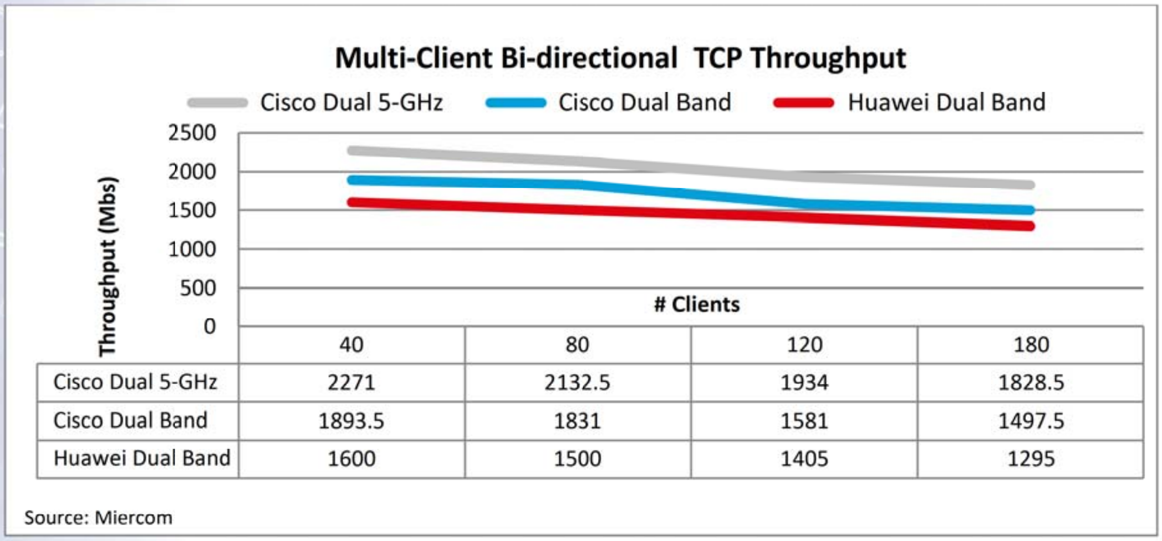
Client Distribution by AP in 5 GHz (Total of 140 Clients)

AP number	Huawei Dual-Band	Cisco Dual-Band	Cisco Dual 5-GHz
1	30	36	20
2	46	20	43
3	27	29	33
4	3	12	11
5	14	21	21
6	20	22	12

Huawei's active AP client count varied from 3 clients on one AP, up to a substantial load of 46. With Cisco's comparable dual band configuration, the AP client count ranged from a low of 12 clients on one AP, up to 36 on the heaviest loaded – a much more reasonable distribution.

Throughput Performance

Using Ixia's IxChariot test tool, we ran throughput tests to measure how much aggregate throughput could be achieved through each vendor's infrastructure to and from the same wireless clients. Representing typical user traffic today, bi-directional, connection-oriented TCP traffic was applied. Tests were conducted with 40, 80, 120 and all 180 clients, using the same 5 GHz and 2.4 GHz client mix. We constrained the Cisco APs' FRA (Flexible Radio Assignment) feature in order to keep all the Cisco APs operating at 5 and 2.4 GHz (dual mode). When enabled and running, FRA would automatically flip two Cisco APs' 2.4-GHz radio to operate at 5 GHz. This "Cisco Dual 5 GHz" scenario delivered the best throughput performance.



	40	80	120	180
Cisco Dual 5-GHz	2271	2132.5	1934	1828.5
Cisco Dual Band	1893.5	1831	1581	1497.5
Huawei Dual Band	1600	1500	1405	1295

Source: Miercom

The Cisco dual 5-GHz configuration achieved 41.8 percent more aggregate bi-directional throughput than the Huawei infrastructure with 40 active clients. With 180 clients Cisco delivered 41 percent more throughput. When constrained to dual-band operation, the Cisco advantage dipped but was still significant, delivering 22 percent more throughput with 80 active clients and 15.6 percent more with the full load of 180 clients.

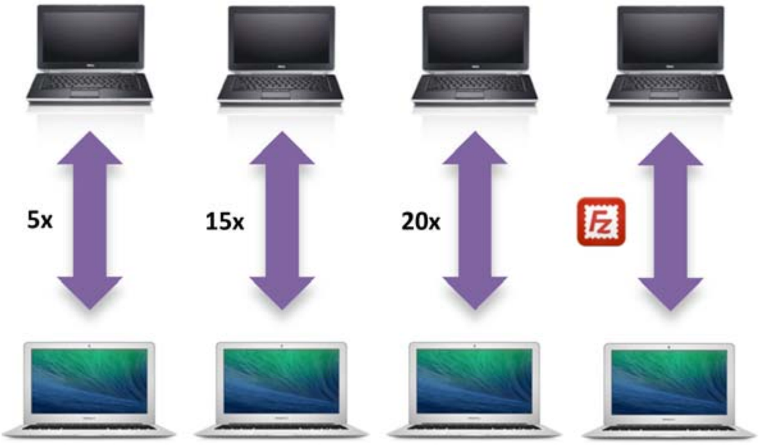
Packet Loss with Huawei

We observed another difference between the Cisco and Huawei environments. The same bi-directional throughput tests yielded some packet loss where some clients did not transmit/receive traffic, but only with the Huawei infrastructure. Packet loss was not substantial, although it increased measurably with the number of active clients. Recurring packet loss to any extent causes performance issues because lost packets have to be identified and resent. The fact that there was no corresponding packet loss with either Cisco configuration makes this observation notable.

QoS Support for Video Calls

We ran tests to ascertain the wireless infrastructures' ability to prioritize traffic. This testing involved the 24 wireless clients in the cubicles served solely by the fifth AP. An Apple MacBook and iPhone were in each of the cubicles.

QoS was enabled in the wireless infrastructure to give priority to video streams following vendor best practices. Then a continuous repeat of a 10 GB file was sent over FTP to wireless clients to apply background load. Jabber video calls, with a continuously moving fractal pattern in the video background, were then launched between PCs and Macs. Testers walked around and judged the "watch ability" of each video call. There were a few minor glitches in some of the videos, but the determining factor in a successful run of video calls was that no calls were dropped.

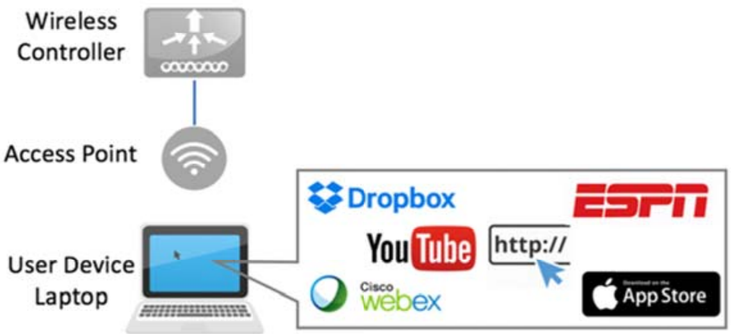


Source: Cisco

We began with Jabber video sessions to five clients, which ran without issues with Huawei and Cisco. Then we ran the test again with 10, 15 and finally 20 clients, noting when video calls were unwatchable or the video-feed connections dropped. The Huawei AP could sustain a maximum of 11 completely successful concurrent Jabber video calls. The Cisco AP, however, could sustain 18 concurrent Jabber calls without issues.

Application Visibility & Control

The Cisco and Huawei infrastructures we tested both included the ability to analyze traffic, a necessary first step in identifying traffic threads that could pose a threat. In its literature Huawei claims it can identify traffic from many applications. In testing, though, we found that Huawei's traffic recognition in many cases stops at a high level (for example, identifying traffic as http/https, which is the basis for nearly all Web browsing). Consequently, without identifying more traffic specifics, visibility and subsequent control of traffic streams is limited.



Source: Cisco

The below table shows the results of some traffic streams we sought to identify in our testing. Where the specific traffic source could be identified a "yes" is shown. A "no" is shown in some cases for Huawei; the message could be seen but Huawei couldn't distinguish the particular source due to a lack of a deep packet inspection.

Category	Application/Source	Huawei	Cisco
Web	ESPN	Yes	Yes
	BBC	Yes	Yes
	Fox News	No	Yes
	YouTube	Yes	Yes
	Instagram	No	Yes
	Speed Test	No	Yes
Meeting	WebEx	No	Yes
	WebEx Screen Sharing	No	Yes
File Sharing	Dropbox	No	Yes
iOS update	iOS-app-download	No	Yes

We observed that Cisco does a deeper dive into traffic and is able to better detail suspect traffic sources through deep packet inspection, or DPI. Cisco also is more adept at profiling and recognizing encrypted packet streams.

Client Profiling

Network security today requires the ability to readily identify traffic sources that could pose a threat. We tasked the Cisco controller with characterizing the type of wireless devices connected to APs in our test bed. The Cisco dashboard displayed the following device identities:

Reported Identity	Actual Wireless Device Type
OS_X-Workstation	MacBook
Microsoft-Workstation	PC (MS Windows 10)
Apple-iPhone	Apple iPhone
Android-Google	Nexus 5X Android smartphone

Huawei does not support this client-profiling capability.

Interference Detection and Identification

Both Cisco's and Huawei's wireless infrastructures include applications and tools for reportedly identifying sources of wireless interference. For this test we introduced a number of common devices well known to interfere with wireless frequencies and operation. These included: a Bluetooth wireless speaker, a microwave oven, a video camera, and a Jammer – built specifically to interfere with wireless networks. Then, using the available features of each vendor's wireless infrastructure, we ascertained how well the products could identify the sources of interference. The results are shown below.

Actual Interference Device	Cisco: Detect and Recognize?	How did it identify and report?	Huawei: Detect and Recognize?	How did it identify and report?
Bluetooth speaker	Yes	"BT Link"	No	N/A
Microwave oven	Yes	"MW Oven"	No	N/A
Video camera	Yes	"Video Camera"	Limited*	"unknown fixed frequency" device
Jammer	Yes	"Jammer"	No	N/A

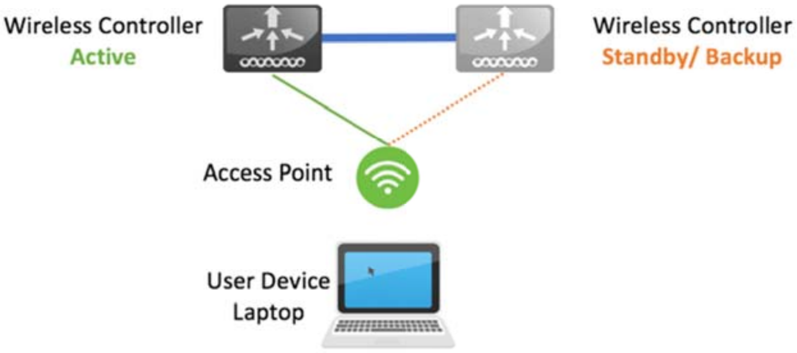
*Huawei didn't detect any interfering devices that were 30 feet or further away from the AP. The video camera was detected as "unknown fixed frequency" device when running 4 feet from the AP.

High Availability

Both vendors offer so-called High-Availability (HA) solutions, to minimize the effect of a single link or device failure. We conducted tests to ascertain the relative effectiveness of these offerings in preserving uptime for wireless clients.

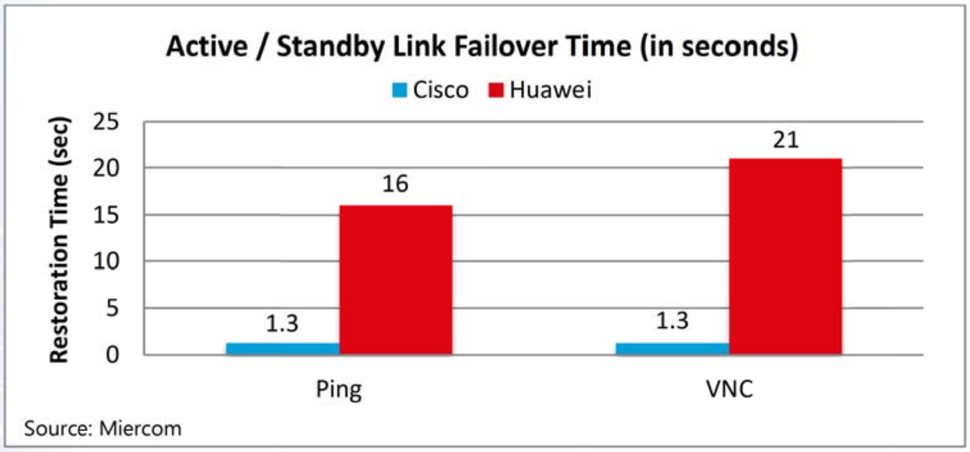
As part of its HSB (Hot Standby) offering, Huawei allows two wireless Access Controllers (ACs) to be configured in an active/standby mode, to which the APs are dual-homed through an access switch. To expedite failover, user information is backed up on the standby AC. When the active AC recovers, operations and services are switched back over with minimal interruption.

Cisco similarly allows two of its WLCs (Wireless LAN Controllers) to be redundantly deployed. In addition, we noted that Cisco offers other reliability enhancements, such as fast system restarts; redundant 1-gigabit or 10-gigabit connectivity; solid-state storage with no moving parts; and optional, redundant, hot-swappable power supplies.



Source: Cisco

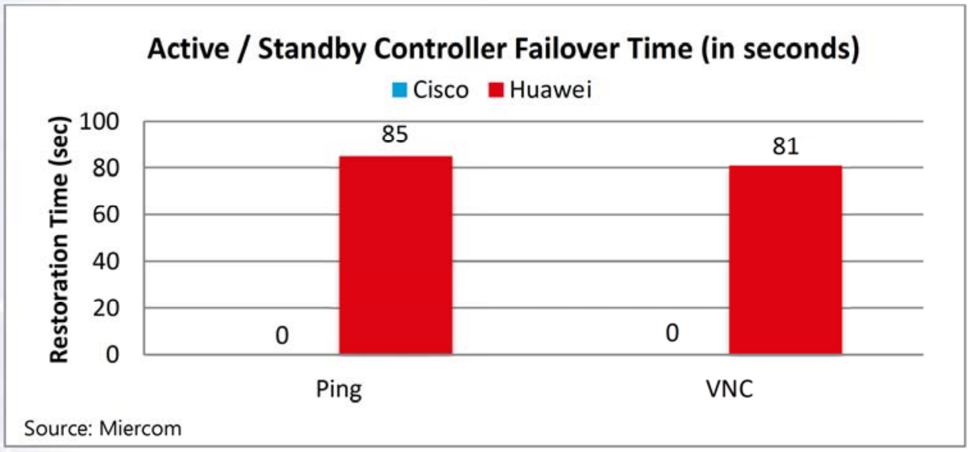
We first tested loss of the active link between controllers (switch/port failure), prompting switchover to the redundant link. We did this while running two applications between devices connected through the disconnected link to see how long it took these apps to restore connection. These applications were a 0.1-second continuous fast ping and a VNC video stream. The chart below shows the time, in seconds, to restore the application connection.



Source: Miercom

Cisco showed significantly faster recovery time. Cisco had 14.7 seconds faster in recovering application connection for a ping than Huawei. The failover time for the VNC video stream was 19.7 seconds faster for Cisco than Huawei.

In a second test, we power-failed the active controller, prompting a failover to the standby, while running the same ping and VNC Video apps.



Source: Miercom

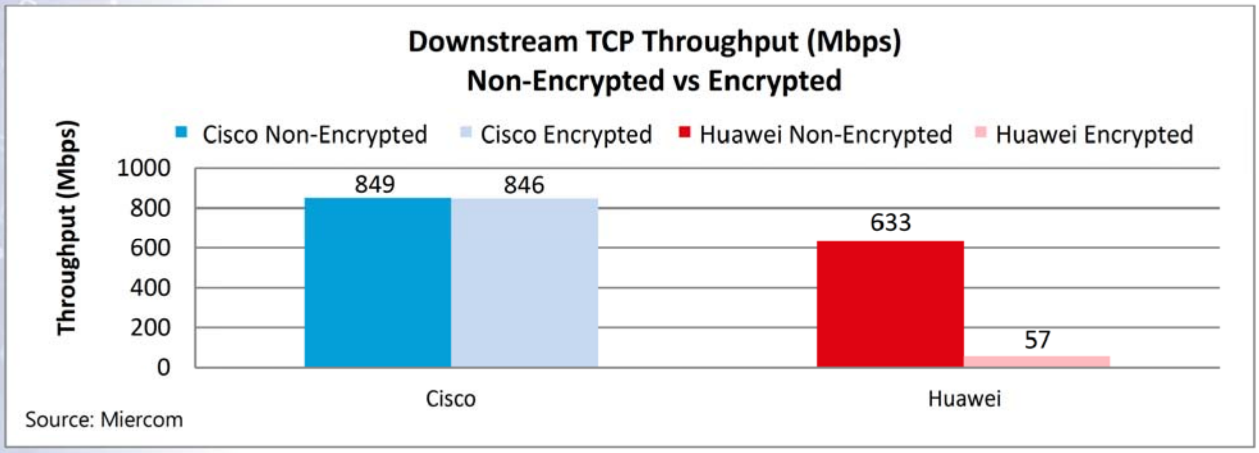
Cisco saw no interruption to these applications during failover. Huawei saw as much as 85 seconds of restoration time.

We found the Cisco's Stateful Switch Over (SSO) architecture was responsible for restoration time, by saving port states in hardware as the controller goes down. The actual Cisco switchover time is less than a second, making application failover time imperceptible to end users.

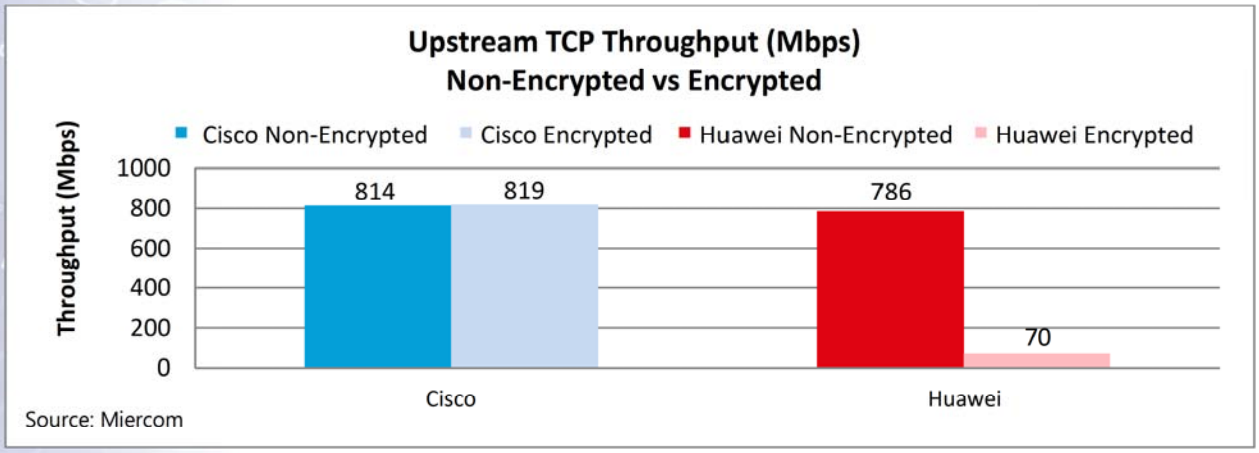
DTLS Encryption

A protocol called DTLS, for Datagram Transport Layer Security, is designed to prevent eavesdropping, tampering and message forgery and is used increasingly for securing wireless transmissions. With other security mechanisms, DTLS also entails encryption of the message payload. This is typically done by the AP for outgoing wireless messages.

We conducted tests measuring AP throughput for TCP traffic. We first sent unencrypted traffic out to wireless clients, shown in the below chart as "TCP Down" with "DTLS Off." We also measured "TCP Up" throughput, for traffic back to the AP from wireless clients. Then we repeated the test, this time after enabling DTLS encryption. As shown, Huawei's throughput dropped precipitously, to only about 10 percent of unencrypted throughput.



Source: Miercom



Source: Miercom

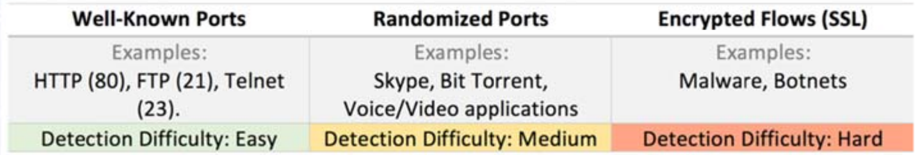
Cisco's encryption throughput saw little degradation due to its specialized encryption hardware. Huawei's APs, by comparison, perform encryption processing using software which applied a heavy load, decreasing throughput by as much as 90 percent.

4 - Wired

Encrypted Traffic Analytics

Today, it's essential to know the traffic or data used by applications within your network. The applications, users, time of use and, most importantly, safety and compliance are vital information for organizational policies.

There are a variety of applications in the today's networks:



Well-Known Ports	Randomized Ports	Encrypted Flows (SSL)
Examples: HTTP (80), FTP (21), Telnet (23).	Examples: Skype, Bit Torrent, Voice/Video applications	Examples: Malware, Botnets
Detection Difficulty: Easy	Detection Difficulty: Medium	Detection Difficulty: Hard

Source: Cisco

As applications, users and devices are evolving beyond using standard ports and flows, infrastructure vendors must make their products and services more intelligent to detect, identify and control every packet flowing through the network. There are various standardized procedures and protocols for collecting specific packets and data streams arriving on network interfaces. Cisco AVC (Application Visibility & Control) uses DPI (Deep Packet Inspection) and heuristic based analysis to identify granular application flows and sub-flow across its wired, wireless and routing platforms. Similar to Cisco AVC, Huawei also offers SAC (Smart Application Control) in wireless but it is not available on their switches.

By aggregating the application flow information from infrastructure devices via NetFlow in Cisco StealthWatch, a network administrator can identify the source/ destination of traffic, class of service, and similar aspects of network traffic. Huawei also supports flow aggregation via NetStream.

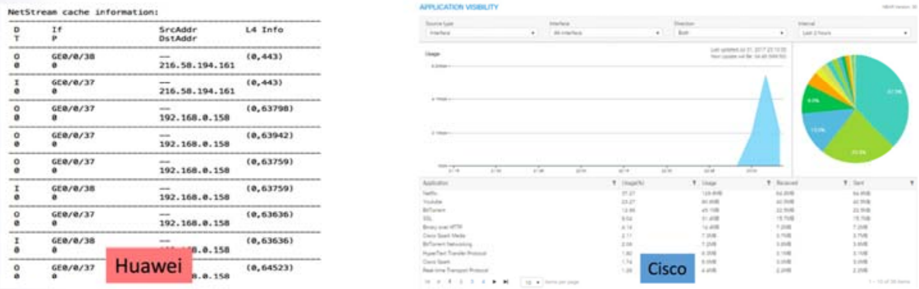
Recently the number of encrypted applications is growing exponentially. These applications are difficult to identify because network devices cannot look inside encrypted traffic, either because of the technical issues or privacy concerns. Malicious users are taking advantage of this opportunity to hide malware, botnet or Trojans inside encrypted traffic to send malicious packets across networks, leaving network administrator completely blind about potential threats hidden inside encrypted flows. Cisco can identify threats inside encrypted traffic with its new technology – ETA (Encrypted Threat Analytics). Cisco StealthWatch with Cognitive Threat Analysis uses a multi-layer machine learning algorithm and various other techniques like packet timing, packet sequence and initial packets stamps to identify threats inside encrypted traffic without infringing the data privacy.

In our comparative analysis, we found Cisco implements AVC and NetFlow in a hardware ASIC (application-specific integrated circuit), which means NetFlow captures do not sap power from the main switch processors.
We compared Cisco and Huawei's technologies in three key test cases of traffic analysis:

1. Port based traffic identification
2. Application level visibility
3. Threat detection in encrypted traffic

Results:

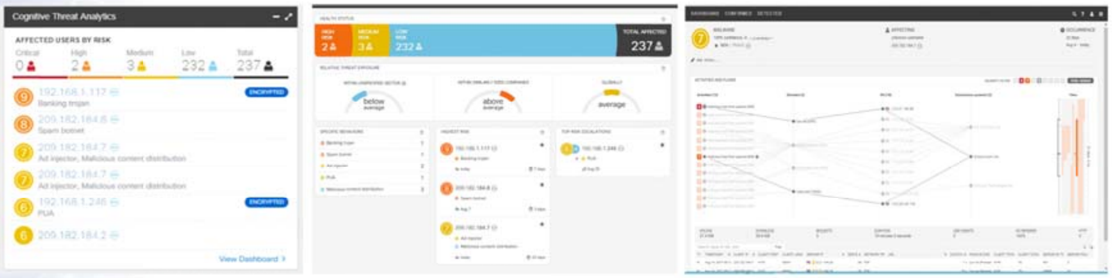
In the first two test cases, Huawei only identified applications based on standard port numbers, such as HTTPS (443). Huawei failed to provide any insights on applications like WebEx, YouTube, BitTorrent, Netflix, Spark and Skype. Moreover, Huawei did not offer any web interface to monitor this traffic. In contrast, Cisco offered intuitive web dashboard (and CLI) to identify applications by port number and by names (YouTube, BitTorrent, Netflix, Spark Media).



```
NetStream cache information:
--------------------------------------------------------------
D      If                  SrcAddr             L4 Info
T      P                   DstAddr
--------------------------------------------------------------
O      GE0/0/38            —                   (0,443)
0      0                   216.58.194.161
--------------------------------------------------------------
I      GE0/0/37            —                   (0,443)
0      0                   216.58.194.161
--------------------------------------------------------------
O      GE0/0/37            —                   (0,63798)
0      0                   192.168.0.158
--------------------------------------------------------------
O      GE0/0/37            —                   (0,63942)
0      0                   192.168.0.158
--------------------------------------------------------------
O      GE0/0/37            —                   (0,63759)
0      0                   192.168.0.158
--------------------------------------------------------------
I      GE0/0/38            —                   (0,63759)
0      0                   192.168.0.158
--------------------------------------------------------------
O      GE0/0/37            —                   (0,63636)
0      0                   192.168.0.158
--------------------------------------------------------------
I      GE0/0/38            —                   (0,63636)
0      0                   ...0.0.158
--------------------------------------------------------------
O      GE0/0/37                                (0,64523)
0      0                   ...0.0.158
```

Source: Cisco

In the third test case, Huawei completely failed to offer visibility on threats inside encrypted traffic. For Huawei, all the traffic was identified as SSL/TLS traffic with no insight about the malware and botnet hidden inside the encrypted traffic. Cisco accurately identified the threats hidden inside encrypted traffic and took necessary action to mitigate those threats.



Cognitive Threat Analytics

AFFECTED USERS BY RISK

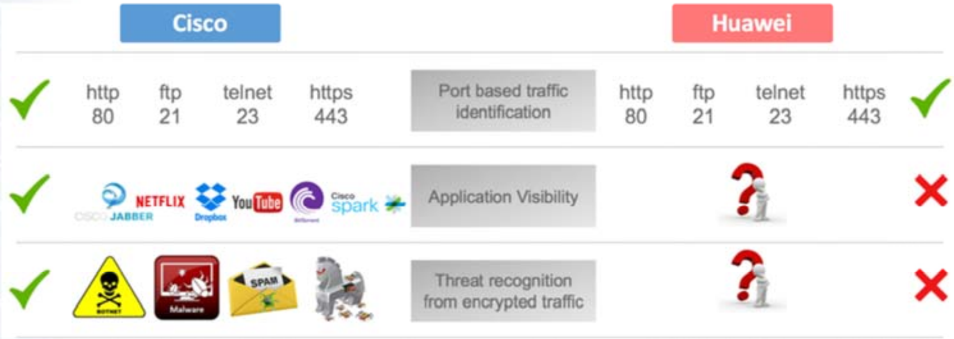
Critical	High	Medium	Low	Total
0	2	3	232	237

- 9 192.168.1.117 — Banking trojan — ENCRYPTED
- 8 209.182.184.6 — Spam botnet
- 7 209.182.184.7 — Ad injector, Malicious content distribution
- 7 209.182.184.7 — Ad injector, Malicious content distribution
- 6 192.168.1.246 — PUA — ENCRYPTED
- 6 209.182.184.2

View Dashboard >

Source: Cisco

To summarize, from basic visibility to robust security, Cisco successfully delivers innovative tools for enterprises to identify application flows, offer strong security and compliances to their network infrastructure. Huawei solutions lack the same level of visibility and security required for modern application and threats.



	Cisco		Huawei	
✓	http 80 ftp 21 telnet 23 https 443	Port based traffic identification	http 80 ftp 21 telnet 23 https 443	✓
✓	CISCO JABBER NETFLIX Dropbox YouTube BitTorrent Cisco spark	Application Visibility	?	✗
✓	BOTNET Malware SPAM	Threat recognition from encrypted traffic	?	✗

Optimized and Secured Switching Resources

With the emergence and growth of IoT markets, there is a growing need for security and segmentation. The network needs to correctly identify and provide controlled-access for users and devices. Regardless of the communication medium, today's world consists of dynamic access through automated policy. The network infrastructure must support programming of its resources both dynamically and statically. Network policy constructs are applied in the form of Security ACLs and QoS Filtering to physical and logical ports such as L2 VLANs, or L3 Routed Access interfaces.

Miercom tested and compared the hardware capabilities of the Cisco and Huawei Campus switches. The Huawei S5720-HI switch was compared against the Cisco Catalyst 9300 and 3850 switch series. This was a multi-purpose test to assess the switch policy filter scalability limits and resource management. Additionally, each switch was tested to determine if it would be susceptible to a network security breach during modifications to an existing policy filter.

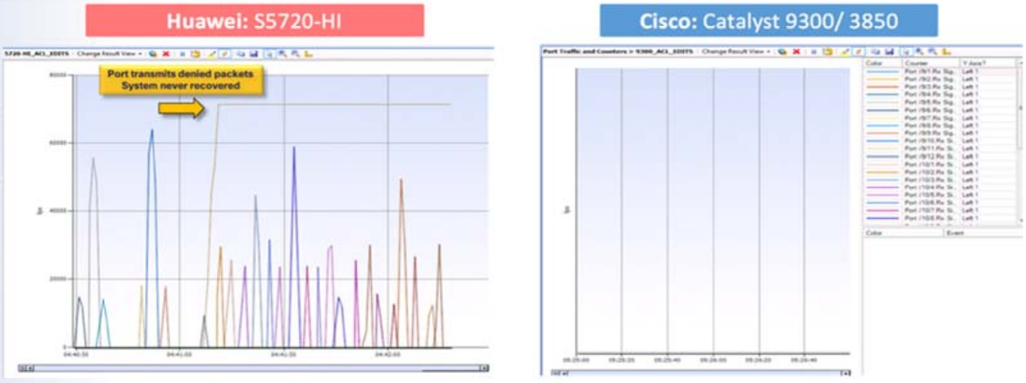
We compared Cisco and Huawei security filtering in four test cases:

1. When applying the same ACL to multiple interfaces, does the ACL consume N x TCAM entries, where N is the number of ports to which the ACL is applied?
2. Does the switch support optimized resources - ACL Sharing?
3. How does the switch manage changes to the existing ACL?
4. Does the switch allow denied traffic to be forwarded during ACL editing?

Each switch was configured with a single ACL Policy configured with 300 rules. Inbound and outbound policies were applied to each L3 interface. A Spirent Test Center was connected to each switch for traffic generation and with PCs connected to each switch to test access to services such as FTP, ICMP, Telnet, and SSH. The switches were monitored for resource utilization such as TCAM, CPU usage, ALC counters, and system logging.

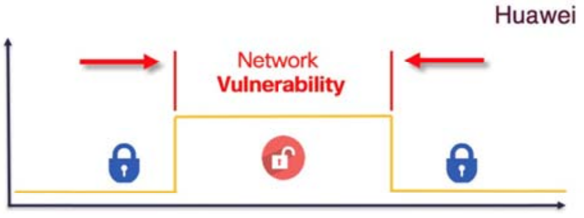
When applying the same ACL to multiple interfaces, the ACL consumed N x TCAM entries, where N was the number of ports to which the ACL was applied. For example, on the Huawei S5720-HI, an inbound ACL with 300 rules applied to all ports (48 southbound interfaces and 4 uplink interfaces) consumed 15,600 rules. When attempting to apply the same ACL for outbound direction, the S5720-HI was limited to only a subset of interfaces as it completely exhausted the hardware resources of the Huawei Switch. Huawei's resource allocation was not optimized and did not offer scalability for this test case. Their documentation recommends the user to merge rules, change a hardware resource template or switch to a VLAN-based approach.

When applying the ACL to all 48 ports of the S5720-HI, the switch exhibited significant time (in minutes) for the ACLs to become active. When editing an ACL on the S5720-HI, the implementation behavior appeared flawed and had exposed the network to a security breach. Due to the architecture of the switching resources, the Huawei 5720-HI switch "allowed" denied traffic to forward during an ACL edit. When edits were made, the old security policy was removed from switch hardware resources. The switch then reprogrammed the resources with the revised statements. Not only did this take a long time, but it left the network vulnerable.



Source: Cisco

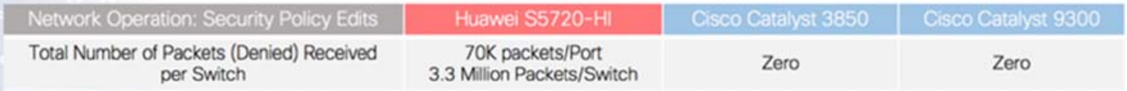
During the policy edits, the PC successfully downloaded a file from the FTP server which had an ACL rule to block FTP traffic as part of the configured policy.



Source: Cisco

The S5720-HI also allowed thousands of denied packets on every switch port. The Spirent system reported that, by the time the ACL change took effect on all ports on the Huawei switch, 70,000 packets had leaked through each switch port – more than 3.3 million packets that should have been blocked. This is a policy violation and window of opportunity for a security breach.

The same set of tests was performed on the Catalyst 3K/9K series switches. The Catalyst switching resources supported high-speed policy edits (add/delete) with efficient resource allocation for scale and secure implementation. With features such as "ACL Label-Sharing" and "Hitless ACL updates", the switches demonstrated programming of policy to the network without being compromised.



Network Operation: Security Policy Edits	Huawei S5720-HI	Cisco Catalyst 3850	Cisco Catalyst 9300
Total Number of Packets (Denied) Received per Switch	70K packets/Port 3.3 Million Packets/Switch	Zero	Zero

Source: Cisco

An ACL is one of the most basic mechanisms used for traffic classification. It can be used for multicast, QoS, and security. It is critical that modifying entries for a specific use case does not affect other operational uses cases for customers. While Cisco passed this test, Huawei failed to meet this important requirement.

Switch Power for Connected Devices

One of the major reasons for network downtime is power interruption. Assuring that network-infrastructure equipment and attached devices continue to function in the event of a power-supply failure is one main way to mitigate this problem. As the Power over Ethernet (PoE) standard evolved to offer more and more power from PoE (15.4W), PoE+ (30W), UPoE (60W) and over 100W (in future), we are seeing influx of devices connecting to the switchport for accessing power and data. In the typical organization, we see traditional PoE devices (IP phones, video cameras, wireless access point) and a new generation of IoT devices (connected LED lights, sensors). The continuous operation of devices such as lights and surveillance cameras is extremely critical.

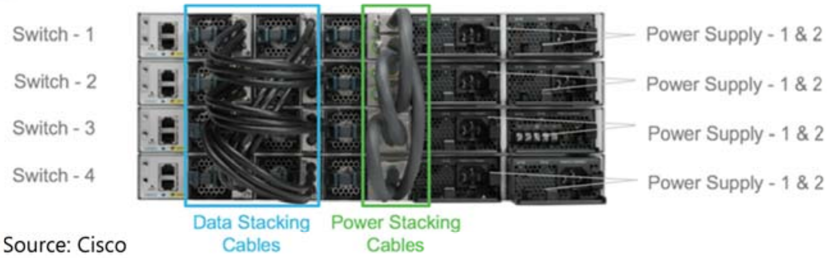
Cisco is making tremendous efforts to offer high availability and uninterrupted power to these devices, even when the switch powering these devices loses some of its power supply units (PSU) or is rebooting or upgrading software. Huawei claims to offer some similar features to Cisco, like decoupling power circuitry with switching hardware or faster power negotiations, but they fall short in real world enterprise deployments.

Our testing of comparative power-supply techniques and processes examined two aspects:

1. Delivering redundant power to switch stacks
2. High Availability for power (Faster PoE provision and uninterrupted power)

Stack power

We observed that a Cisco switches stack can share all the connected power supplies by using special power stacking cables. With the help of this Cisco Stack-Power technology, the need for a separate, external redundant power supply is eliminated, saving time and space. Specific switches and ports, such as with attached PoE devices, can be assigned priority for higher availability during outages.



Source: Cisco

e tested Cisco's Stack-Power by building a switch stack with a single redundant power supply and connecting the following devices: a wireless AP, wired and wireless laptops, an iPhone and various PoE-connected lights. Data was continuously sent to the laptops and iPhone, as we disabled one power supply at a time to see the effect on attached devices. We found that as long as the stack of switches has enough power to power them, they will provide remaining power to PoE devices. Since it was a shared pool of power, it didn't matter which particular power supply was operational or not.

Huawei failed to offer such power pooling capability. The only alternative for Huawei was to add another redundant power supply appliance per 4-6 switches which increases capital, in terms of purchase cost and space requirement, and operational cost for maintaining and monitoring underutilized power supply systems.

High Availability of PoE Power

Cisco offers two high-availability options for devices attached to and powered by Cisco switches: Fast PoE (FPoE) and Perpetual PoE (PPoE).

With Fast PoE, the switch remembers the wattage requirement of the last power drawn on a particular port, and can re-establish PoE power quickly after AC power is restored, without waiting for switch software to fully boot up.

To test Fast PoE, we configured a Cisco 9300 switch for PoE devices, using three LED lights, a wireless access point and an IP phone. Cisco recorded each PoE device's power draw in hardware for possible power-fail events. The switches quickly restored power on resumption of power to the switch, without waiting for switch operating system boot. The switches did not have to re-learn each device's parameters, saving valuable time in bringing up the PoE devices. Our testing found this occurs within 15 to 20 seconds of power restoration.

The same test was then conducted with a similarly configured Huawei switch. When power failure occurred and was then restored, the switch went through its full reboot cycle before re-powering PoE devices. We ran multiple tests and PoE power restoration took an average of 3 minutes, 8 seconds with Huawei, versus 15 to 20 seconds with Cisco, making it nearly 12 times slower than Cisco. This delay was further increased in case of Huawei since even the PoE devices required additional time boot and setup connectivity to network.

Fast PoE	Cisco	Huawei
Average time to restore power to PoE devices	17.5 seconds	3 minutes, 8 seconds

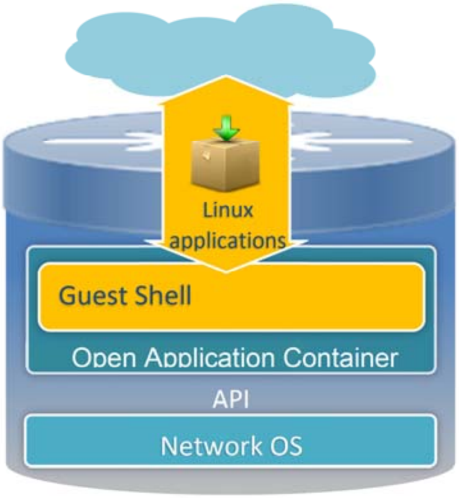
With Cisco's Perpetual PoE (PPoE), power to specified ports is essentially continuous and uninterrupted. To test PPoE, several lights were PoE-connected to Huawei and Cisco switch ports designated as PPoE. Power to the switches was not interrupted as each switch was software-rebooted. The time that the lights went out and came on again was measured. The results below show that with PPoE, devices lost no power after a software-reboot of the Cisco switch, while PoE devices on the Huawei switch lost power an average of 12 seconds. Any power interruption makes connected PoE device reboot which adds up some more downtime which is not acceptable when critical devices connected to the switch.

Perpetual PoE	Cisco	Huawei
Average time lights went out after switch reboot	0 seconds (lights did not go out)	12 second average (varied from 8 to 16 sec)

To summarize, Cisco Stack-Power offers unique advantages over Huawei by pooling power supplies from the individual sources to enable resiliency. Cisco Fast PoE and Perpetual PoE offers high availability to all the PoE connected device when device reboots, either intentionally or unintentionally.

Software Enhancements and Programmability

We noted during our testing that the latest Cisco switch software has evolved from the monolithic IOS of the past, to a more modern and programmable operating system. Cisco switches ran the latest v16.6.1 of IOS XE, which runs IOS functionality as an application atop a Linux kernel. With the Linux kernel, Cisco is able to offer users and developers rich access to a Linux guest shell via numerous programming interfaces, including for application hosting.



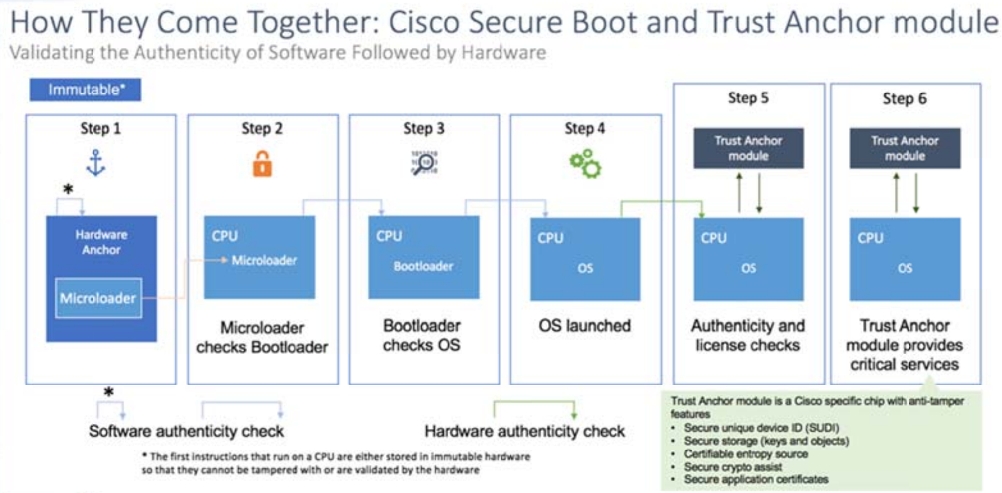
- Cisco's IOS-XE has the ability to host Linux based applications via their Guest Shell feature which can provide a number of valuable use cases for the network infrastructure. Guest Shell allows customers to operate/install popular and common Linux applications (such as: YDK (the Yang Development Kit), Python object-oriented programming, protocol support for NETCONF (the IETF Network Configuration Protocol) and RPC (remote procedure call), and JSON (Java Script Object Notation) and XML encoding, and many more…) in a secure manner, thus enable hosting/running open Linux applications, yet still making sure that they will not harm any critical functionality of the switch (such as rebooting the switch from the shell or tampering with the Kernel or causing any un-expected downtime on the device while in production mode.)
- One of the benefits of a Linux based Guest Shell is allowing customers to use any scripting language available on Linux, to perform basic on-box automation tasks. One of those languages is Python, which is supported as a built-in programming language on Cisco's Polaris Guest Shell.
- To evaluate Guest Shell, we ran an on-box automation script that runs on the switch as an 'agent', and on each configuration change it detects, an email is sent to the admin to notify about the changes detected. We were easily able to configure the Guest Shell Linux to role as an email server from which we were able to automate the email notification between the switch and the admin. We then ran the Python script agent in the Guest Shell.
- While the agent was running, we made several configuration changes on the switch, and the email notifications were sent to the administrator immediately. Via the Python code, we were able to set the e mail address of the admin. In the products evaluated in this report, Huawei has no feature which is equivalent to Cisco's Guest Shell.

5 - Trustworthiness: Securing the Network

We noted, too, several new features that bolster network and system security, and the ability of the user to monitor and identify problems and threats. Key among these are:

- **Image Signing** - where digitally signed software is used to protect against the use of counterfeit images and to assure that the image has not been modified or tampered. The code signing uses a hashing algorithm, similar to a checksum; the hash is then encrypted using a signing key. The signed code is checked at runtime and validated by a trusted system element to ensure it has not changed. The trusted element is a piece of code known to be authentic and is unable to change (immutable).

- **Secure Boot** - which ensures that only authentic Cisco software boots up (through a secure processor, memory, and boot ROM) on the Cisco platform. This enhances image signing by using a hardware trust anchor, also immutable, and prevents many physical possession attacks and part-replacement attacks.


How They Come Together: Cisco Secure Boot and Trust Anchor module

Validating the Authenticity of Software Followed by Hardware

* The first instructions that run on a CPU are either stored in immutable hardware so that they cannot be tampered with or are validated by the hardware

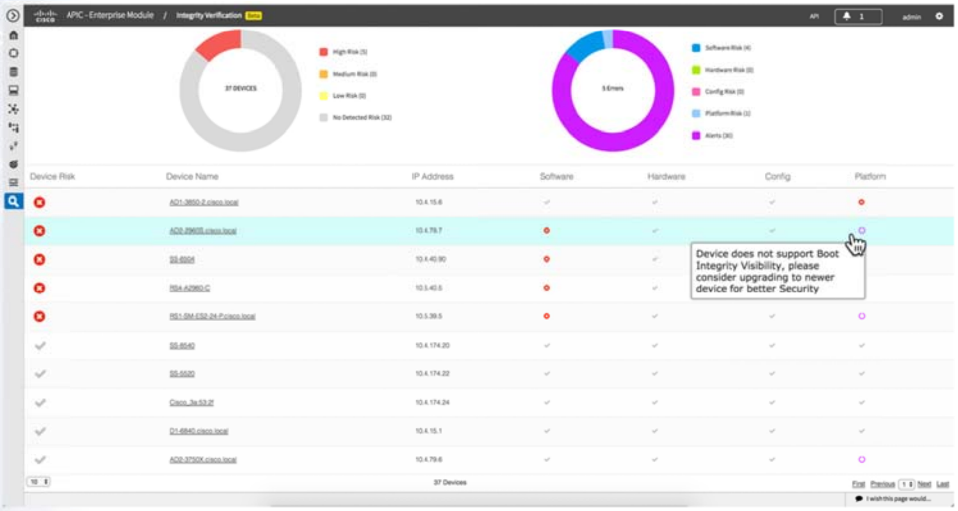
Trust Anchor module is a Cisco specific chip with anti-tamper features
- Secure unique device ID (SUDI)
- Secure storage (keys and objects)
- Certifiable entropy source
- Secure crypto assist
- Secure application certificates

Source: Cisco

- **Trust Anchor Module (TAm)** - is a special anti-theft and anti-tamper chip designed with built-in cryptographic functions that provides both end-user and supply chain protection. End-user protections including highly secure storage of user credentials, passwords etc. whereas Supply-chain protection provides inserting of Secure Unique Device Identifier (SUDI) during manufacturing to validate the authenticity of the hardware – that is genuine Cisco. Unlike generalized solutions like Trusted Platform Module (TPM) that are ideal for general-purpose computing devices like servers and PCs, Cisco TAm is ideal for embedded computing devices like routers and Wi-Fi access points to ensure protection against supply chain and physical-possession-based firmware tampering attacks in conjunction with Secure Boot.

- **Run-time Defenses** - ensures protection against persistent remote Buffer-Overflow and Return-Oriented programming (ROP) attacks by instilling software & hardware development best practices. Cisco practices use of safe libraries and techniques like Address Space Layout Randomization (ASLR), X-Space etc. that makes it extremely difficult for the attacker to guess the memory locations to exploit and thus offering resiliency & mitigation against ROP attacks

Cisco campus-wide networks can also employ APIC-EM – Application Policy Infrastructure Controller - Enterprise Module. This is a unified point for automated management of the whole infrastructure fabric – physical as well as virtual resources. The APIC-EM end-to-end "Trustworthy Dashboard" is part of its "Integrity Verification" module, as shown below, which monitors all levels of the infrastructure.

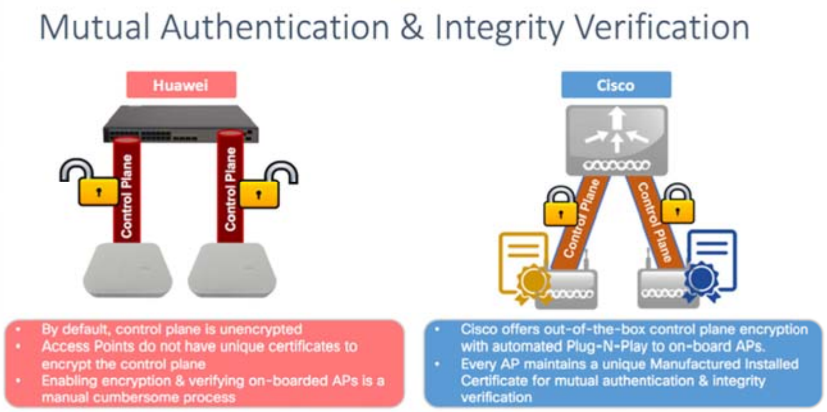


Device Risk	Device Name	IP Address	Software	Hardware	Config	Platform
☒	AD1-3850-2.cisco.local	10.4.15.6	✓	✓	✓	●
☒	AD2-2960S.cisco.local	10.4.79.7	●	✓	✓	○
☒	SS-6504	10.4.40.90	●	✓		
☒	RS4-A2960-C	10.5.40.5	●	✓		
☒	RS1-SM-ES2-24-P.cisco.local	10.5.39.5	●	✓	✓	○
✓	SS-6540	10.4.174.20	✓	✓	✓	✓
✓	SS-6520	10.4.174.22	✓	✓	✓	✓
✓	Cisco_3a:53:2f	10.4.174.24	✓	✓	✓	✓
✓	D1-6840.cisco.local	10.4.15.1	✓	✓	✓	✓
✓	AD2-3750X.cisco.local	10.4.79.6	✓	✓	✓	○

Device does not support Boot Integrity Visibility, please consider upgrading to newer device for better Security

Source: Cisco

- **Control Plane Security** – the communication channel between access points and controller for secure exchange of configurations and wireless client information. By default, Cisco secures the control plane channel by leveraging the unique Manufactured Installed Certificates (MIC) for mutual authentication & encryption, whereas Huawei chooses to keep the control channel unencrypted out-of-the-box. An unsecured channel makes Huawei susceptible to remote replay packet and Man-in-the-Middle attacks that can compromise the identity of the wireless user. Huawei's approach for securing the control plane is manually cumbersome and it's not full-proof either since they rely on using Private Secret Key (PSK) for every Access Point.



Mutual Authentication & Integrity Verification

- By default, control plane is unencrypted
- Access Points do not have unique certificates to encrypt the control plane
- Enabling encryption & verifying on-boarded APs is a manual cumbersome process

- Cisco offers out-of-the-box control plane encryption with automated Plug-N-Play to on-board APs.
- Every AP maintains a unique Manufactured Installed Certificate for mutual authentication & integrity verification

Source: Cisco

6 - Summary

Our evaluation found that, where Cisco and Huawei both offer all the comparable components for building a campus-wide, wireless and wired, network infrastructure, test after test found that the Cisco package offers certain positive advantages that Huawei does not. Cisco showcased superior performance against the Huawei wireless solution with a highly developed resource management, hardware, software and security platform to provide the most optimized, trustworthy system to every customer.

Power and Radio Efficiency. Digging into wireless operations and performance, we found that Cisco efficiently emits lower transmit signal levels than Huawei for the exact same 180-client configuration and deployment. Client connectivity across six AP campus networks was more evenly distributed in the Cisco infrastructure. Most noteworthy is the ability for Cisco APs to automatically switch its 2.4 GHz radio to also operate at 5 GHz for optimal client coverage.

High Performance. Performance testing determined Cisco APs could deliver 15 to 22 percent more aggregate throughput in dual-band mode. When two of the six Cisco APs automatically switched over to dual 5 GHz mode, performance was 40 percent higher.

Video Call QoS and Interference Detection. During active video streaming, Cisco sustained more sessions than Huawei when using the same traffic and client environment. Cisco's ability to correctly detect and identify Wi-Fi interference sources far exceeded Huawei's.

Impressive Failover Handling. High-availability tests found that Cisco offered better failover performance and wireless uptime for users and applications.

Encrypted Traffic Analytics. Cisco successfully delivered innovative tools for enterprises to identify applications and protect network from advanced threats hidden inside encrypted traffic, without compromising privacy.

Secured and optimized hardware resources. Cisco Catalyst switches demonstrated programming of policy to the network without being compromised. We observed that the Huawei switches leaked data that should be blocked during ACL edits.

High Availability for PoE devices. Cisco Stack-Power offers unique advantages over Huawei. Cisco Fast PoE and Perpetual PoE offers high availability to all the PoE connected devices when device reboots, either intentionally or unintentionally

Software Programmability. Cisco IOS-XE Programmability support technologies that simplify automation and provisioning and make the network engineer more efficient.

Trustworthiness. Cisco trustworthy systems establish the base of assurance for an architected secured network.

7 - About Miercom Performance Verified Testing

This report was sponsored by Cisco Systems, Inc. The data was obtained completely and independently by Miercom engineers and lab-test staff as part of our Performance Verified assessment. Testing such as this is based on a methodology that is jointly co-developed with the sponsoring vendor. The test cases are designed to focus on specific claims of the sponsoring vendor, and either validate or repudiate those claims. The results are presented in a report such as this one, independently published by Miercom.

8 - About Miercom

Miercom has published hundreds of network-product-comparison analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

9 - Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Miercom or Cisco Systems, Inc. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.